Attack Patterns

Description

Building software with an adequate level of security assurance for its mission becomes more and more challenging every day as the size, complexity, and tempo of software creation increases and the number and the skill level of attackers continues to grow. These factors each exacerbate the issue that, to build secure software, builders must ensure that they have protected every relevant potential vulnerability; yet, to attack software, attackers often have to find and exploit only a single exposed vulnerability. To identify and mitigate relevant vulnerabilities in software, the development community needs more than just good software engineering and analytical practices, a solid grasp of software security features, and a powerful set of tools. All of these things are necessary but not sufficient. To be effective, the community needs to think outside of the box and to have a *firm grasp of the attacker's perspective and the approaches used to exploit software* [Hoglund 04[1], Koizol 04[2]].

These articles discuss the concept of attack patterns as a mechanism to capture and communicate the attacker's perspective. Attack patterns are descriptions of common methods for exploiting software. They derive from the concept of design patterns [Gamma 95[3]] applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples. Through analysis of observed exploits, the following typical information is captured for each attack pattern:

- Pattern name and classification
- Attack prerequisites
- Description
- Targeted vulnerabilities or weaknesses
- Method of attack
- Attacker goal
- Attacker skill level required
- Resources required
- Blocking solutions
- Context description
- References

This information can bring considerable value for software security considerations through all phases of the software development lifecycle (SDLC) and other security-related activities, including:

- Requirements gathering
- Architecture and design
- Implementation and coding
- Software testing and quality assurance
- Systems operation
- Policy and standard generation

Overview Article

Name	Version Creation Time	Abstract

1. http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/attack/587-BSI.html#dsy587-BSI_hoglund04 (Attack Pattern References)
2. http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/attack/587-BSI.html#dsy587-BSI_koizol04 (Attack Pattern References)
3. http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/attack/587-BSI.html#dsy587-BSI_gamma95 (Attack Pattern References)

Introduction to Attack Patterns	9/30/09 3:26:20 PM	This article is the first in a coherent series introducing the concept, generation, and usage of attack patterns as a valuable knowledge tool in the design, development, and deployment of secure software. It is recommended that the reader also review the following articles to fully understand the context and value of attack patterns.

Most Recently Updated Articles [Ordered by Last Modified Date]

Name	Version Creation Time	Abstract
Introduction to Attack Patterns	9/30/09 3:26:20 PM	This article is the first in a coherent series introducing the concept, generation, and usage of attack patterns as a valuable knowledge tool in the design, development, and deployment of secure software. It is recommended that the reader also review the following articles to fully understand the context and value of attack patterns.
Attack Pattern References	9/30/09 3:03:02 PM	Content area bibliography.
Attack Pattern Generation	11/24/08 10:12:59 AM	This article is the second in a coherent series introducing the concept, generation, and usage of attack patterns as a valuable knowledge tool in the design, development, and deployment of secure software. It is recommended that the reader review the Attack Patterns Introduction article to fully understand the context of the material presented.
Attack Pattern Usage	11/24/08 10:11:36 AM	This article is the third in a coherent series introducing the concept, generation, and usage of attack patterns as a valuable knowledge tool in the design, development, and deployment of secure software. It is recommended that the reader review the preceding articles to fully understand the context of the material presented.

Further Information on Attack Patterns	5/16/08 2:38:58 PM	Further information about Attack Patterns.

All Articles [Ordered by Recommended Reading Order]

Name	Version Creation Time	Abstract
Introduction to Attack Patterns	9/30/09 3:26:20 PM	This article is the first in a coherent series introducing the concept, generation, and usage of attack patterns as a valuable knowledge tool in the design, development, and deployment of secure software. It is recommended that the reader also review the following articles to fully understand the context and value of attack patterns.
Attack Pattern Generation	11/24/08 10:12:59 AM	This article is the second in a coherent series introducing the concept, generation, and usage of attack patterns as a valuable knowledge tool in the design, development, and deployment of secure software. It is recommended that the reader review the Attack Patterns Introduction article to fully understand the context of the material presented.
Attack Pattern Usage	11/24/08 10:11:36 AM	This article is the third in a coherent series introducing the concept, generation, and usage of attack patterns as a valuable knowledge tool in the design, development, and deployment of secure software. It is recommended that the reader review the preceding articles to fully understand the context of the material presented.
Further Information on Attack Patterns	5/16/08 2:38:58 PM	Further information about Attack Patterns.
Attack Pattern Glossary	5/16/08 2:38:58 PM	The Attack Pattern articles use the following terms and definitions.
Attack Pattern References	9/30/09 3:03:02 PM	Content area bibliography.